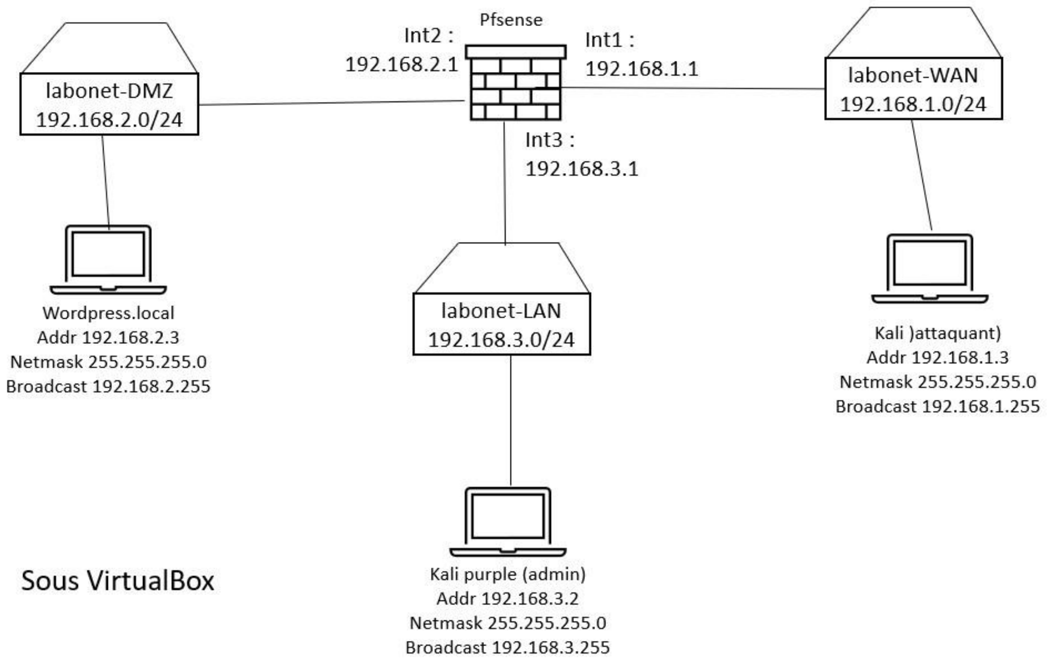
SECS1028 - Laboratoire 9 - Pfsense sous VirtualBox

labo not´e sur 13 points - 10% de la note finale

pour le 31 mars

Objectif du laboratoire : segmenter un r´eseau virtuel sous VirtualBox avec Pfsence

Pour ce Labo, T´el´echarger Pfsense au format ISO et installez le sur une nouvelle VM (avec 10 Go d'espace) disque. Puis connectez les VMs suivant le sch´ema ce-dessous en **r´eseau interne VirtualBox** :



Ip machine virtuell

DMZ(wordpress) : 192.168.2.2

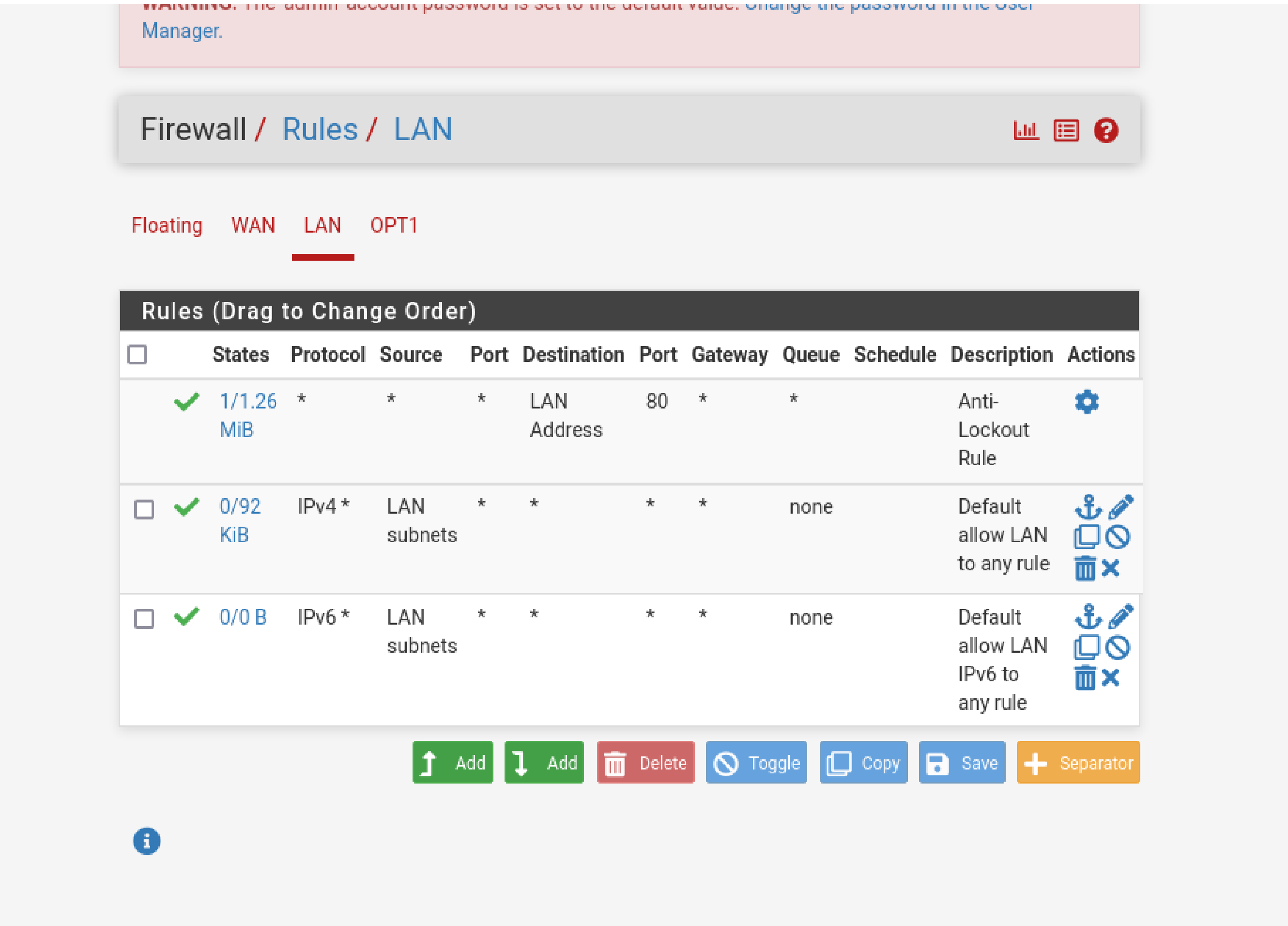
(LAN)Kali purple : 192.168.3.2

(WAN)Kali attaque : 192.168.1.2

1 Installation, configuration et test du r´eseau (5 points)

1) Connectez-vous a` l'interface de pfsense (admin/pfsense (mot de passe `a changer)) via Kali purple. Quelle est la configuration par d´efaut de pfsense sur les 3 interfaces : WAN, LAN et DMZ ? Expliquer pour chaque interface les r`egles de blocages (trafic entrant et sortant) et les ports ouverts ´eventuels. (1 point par interface).

LAN :

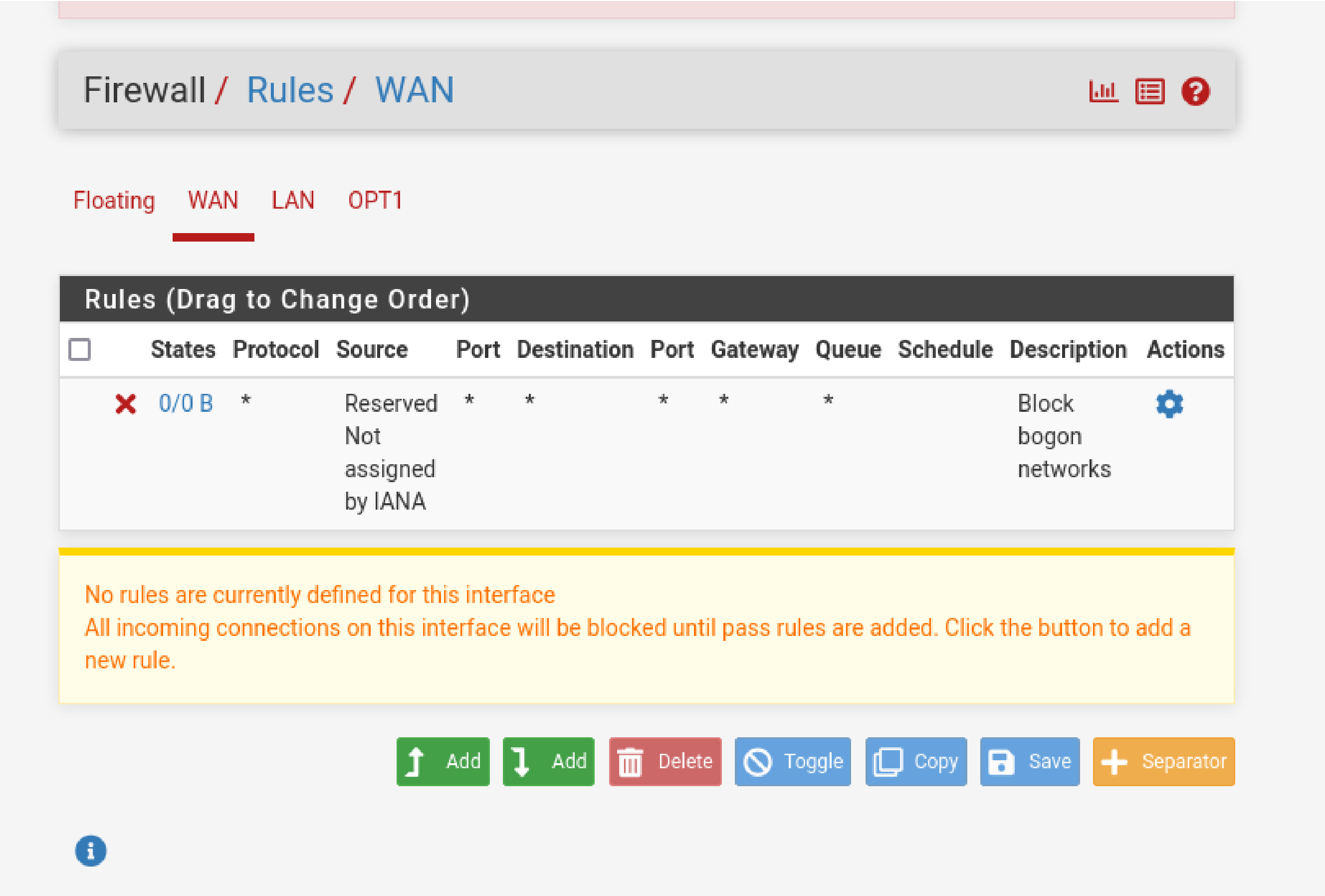


WARNING: The admin account password is set to the default value. Change the password in the User Manager.

Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1/1.26 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
☐	✓	0/92 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
☐	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

WAN :

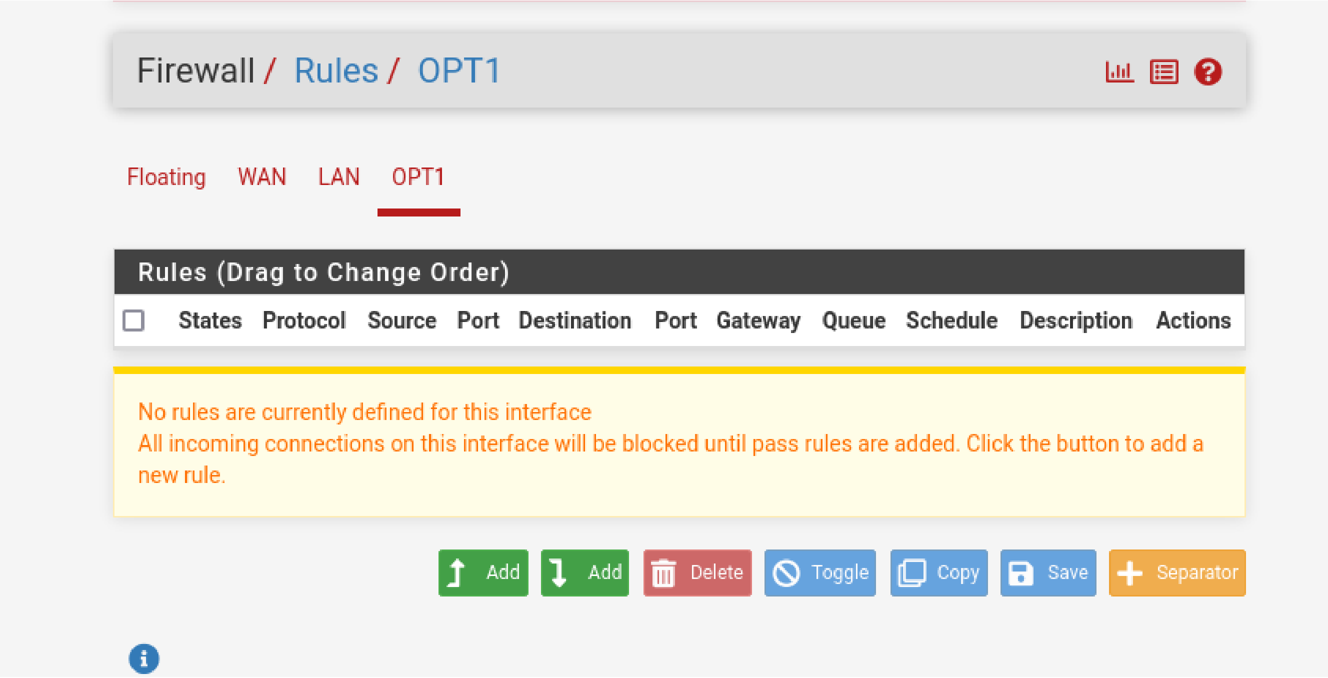


Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

OPT1 :



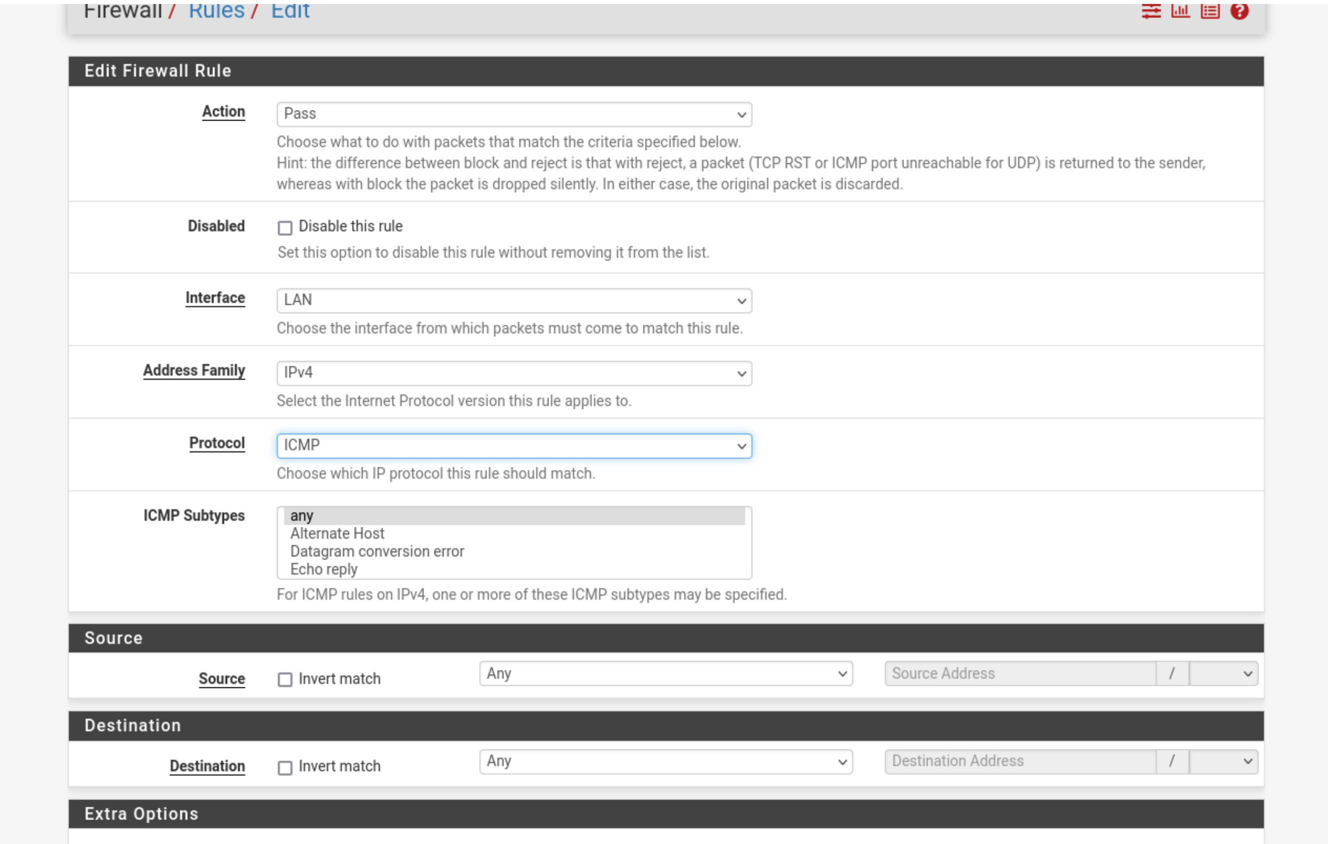
Rules (Drag to Change Order)

□	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

2) Ensuite, configurez pfsense pour laisser passer les requˆetes IPv4 ICMP echo sur l’ensemble du r´eseau du lab. Quelle(s) r`egle(s) avez-vous configur´e ? (capture ´ecran) (1 point).

LAN :



Firewall / Rules / Edit

Edit Firewall Rule

Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	□ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	ICMP Choose which IP protocol this rule should match.
ICMP Subtypes	any Alternate Host Datagram conversion error Echo reply For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

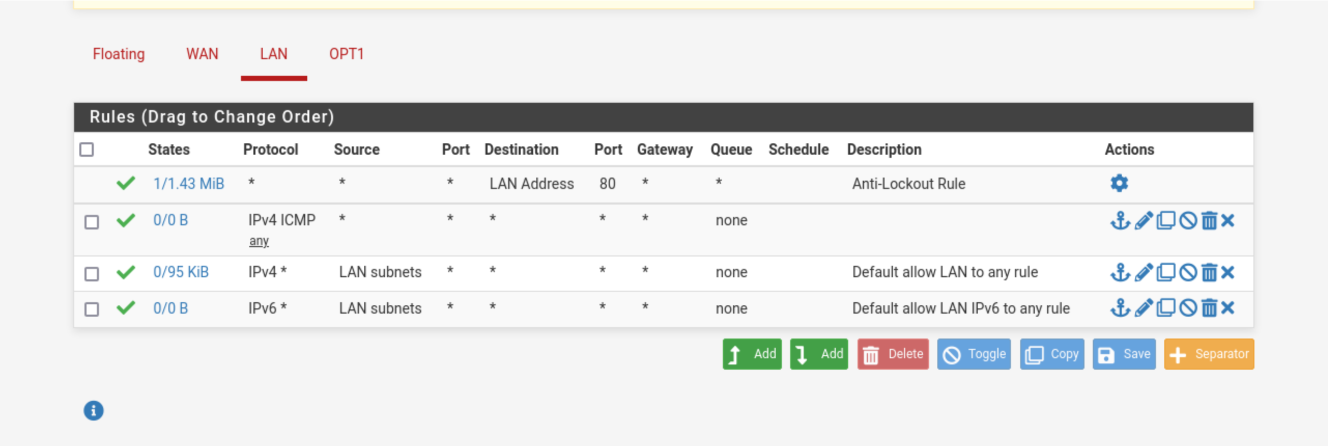
Source

Source	□ Invert match	Any	Source Address /

Destination

Destination	□ Invert match	Any	Destination Address /

Extra Options

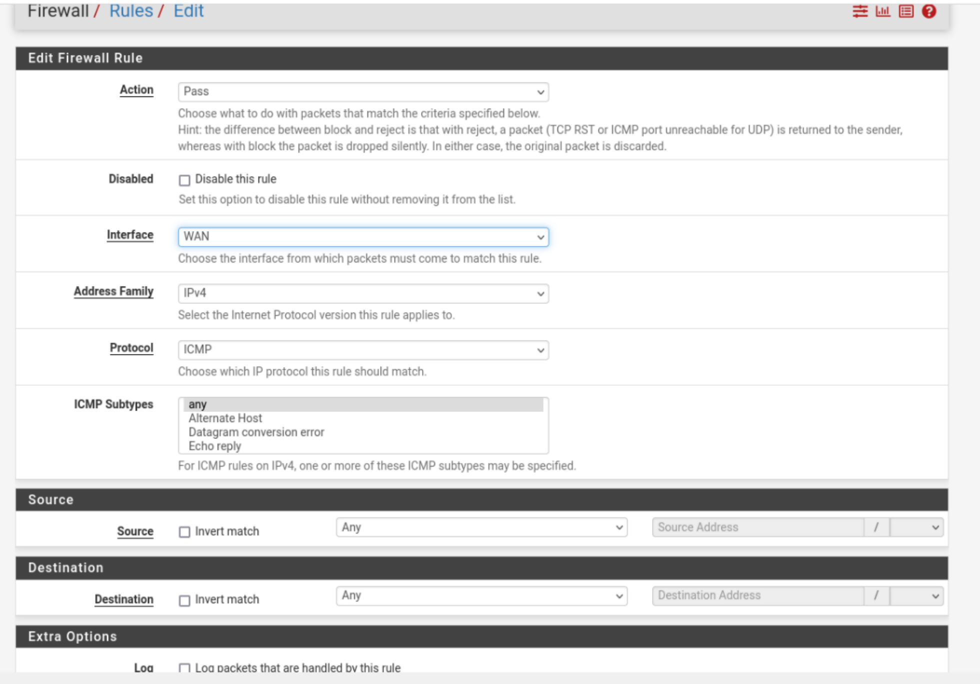


Floating WAN LAN OPT1

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1/1.43 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
□	✓	0/0 B	IPv4 ICMP any	*	*	*	*	*	none			⚓ ✎ ❐ ⊘ 🗑 ✕
□	✓	0/95 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	⚓ ✎ ❐ ⊘ 🗑 ✕
□	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓ ✎ ❐ ⊘ 🗑 ✕

WAN :



Firewall / Rules / Edit

Edit Firewall Rule

Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	□ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	ICMP Choose which IP protocol this rule should match.
ICMP Subtypes	any Alternate Host Datagram conversion error Echo reply For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

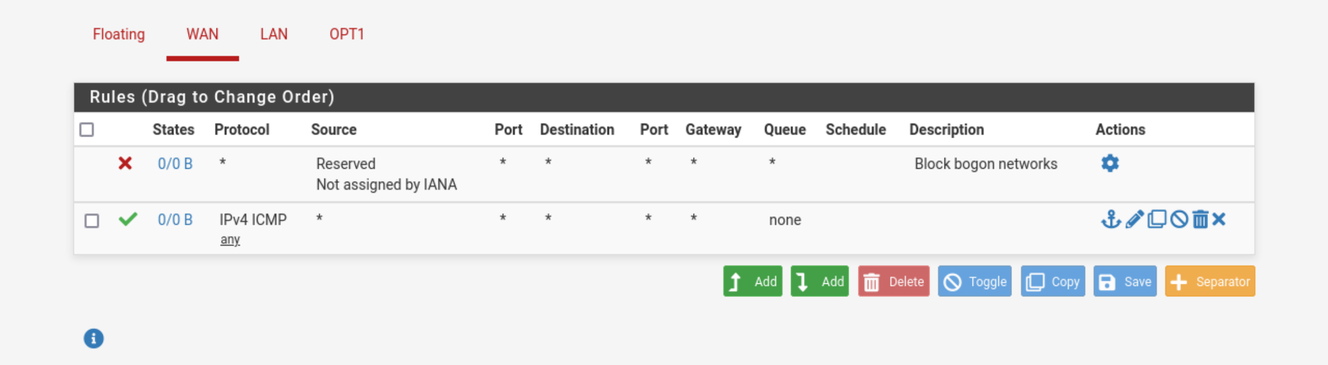
Source	□ Invert match	Any	Source Address /

Destination

Destination	□ Invert match	Any	Destination Address /

Extra Options

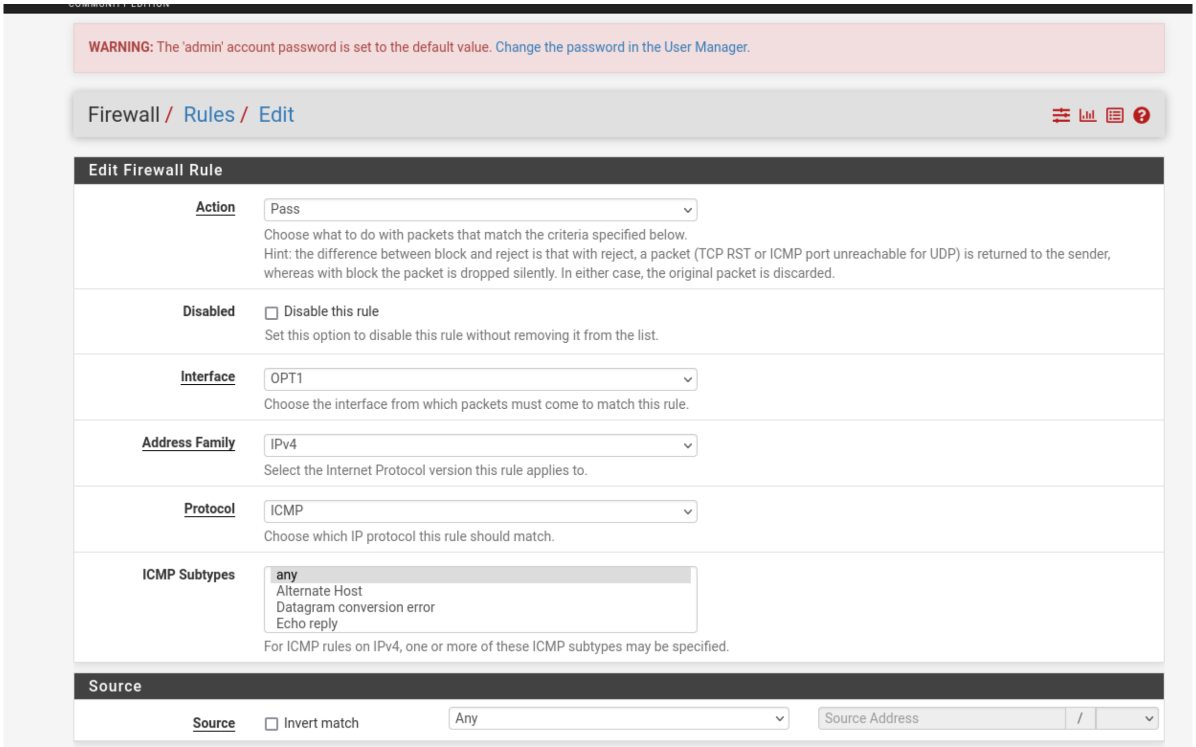
Log □ Log packets that are handled by this rule



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
□	✓	0/0 B	IPv4 ICMP any	*	*	*	*	*	none			⚓ ✎ ⧉ ⊘ 🗑 ✗

OPT1 :



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

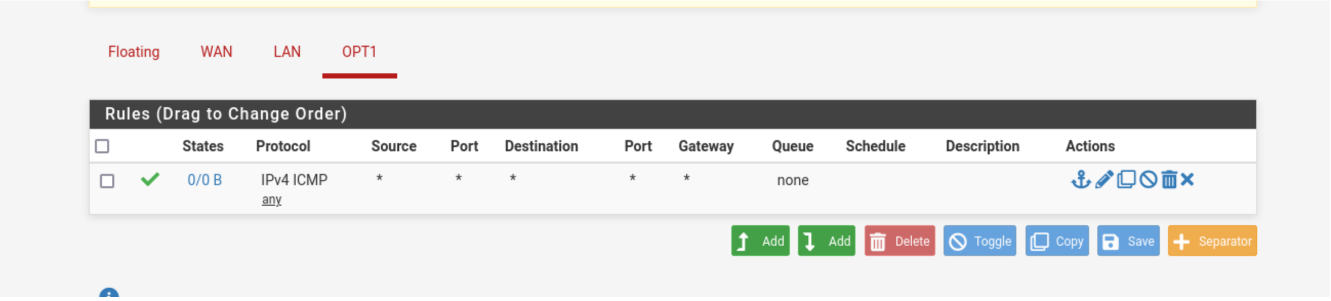
Firewall / Rules / Edit

Edit Firewall Rule

Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	□ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	OPT1 Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	ICMP Choose which IP protocol this rule should match.
ICMP Subtypes	any Alternate Host Datagram conversion error Echo reply For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source	□ Invert match	Any	Source Address /

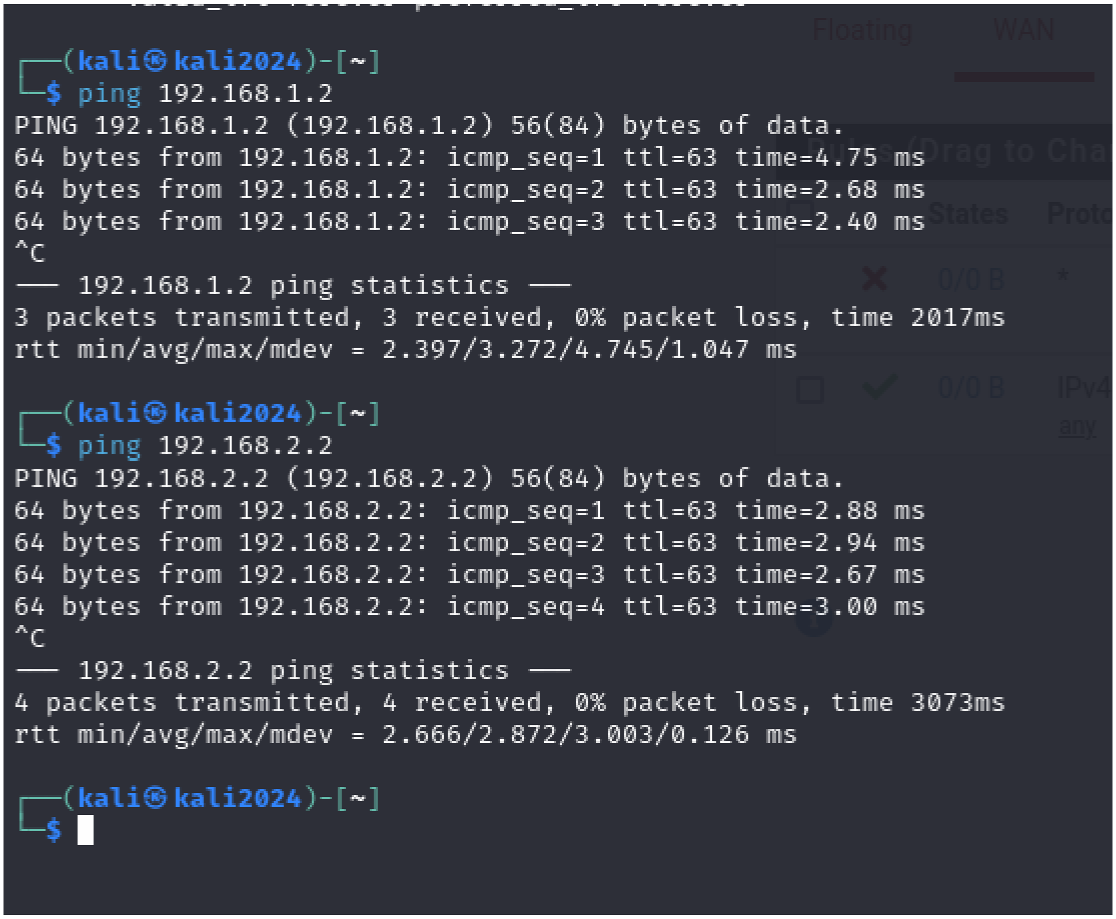


Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0/0 B	IPv4 ICMP any	*	*	*	*	*	none			

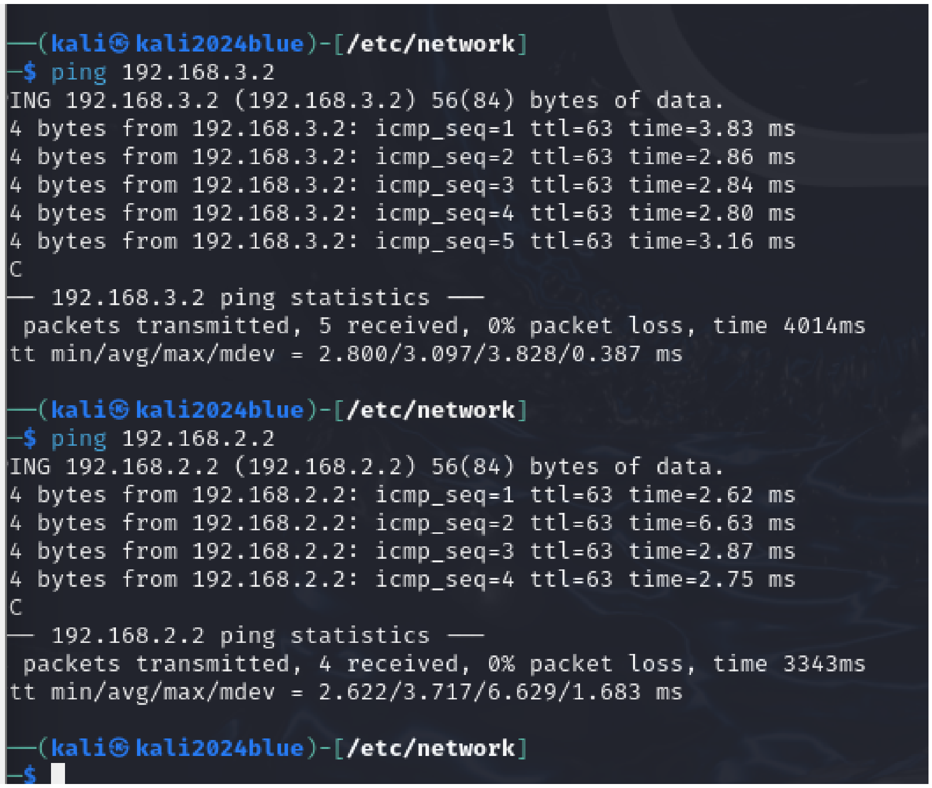
3) Testez les connexions entre les VM en utilisant des requˆetes ICMP echo (ping) IPv4. Montrez par des captures ´ecrans r´eponses des VM aux commandes ping (captures ´ecran): (1 point)

LAN :



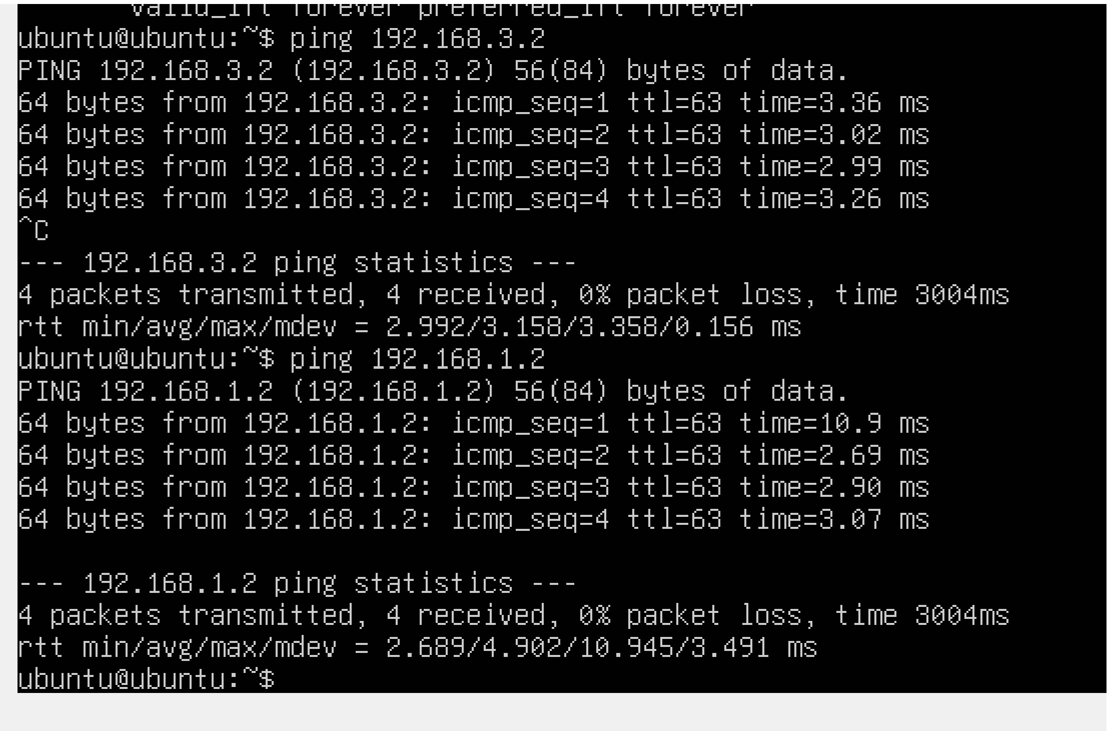
```
┌──(kali㉿kali2024)-[~]
└─$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=4.75 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=2.68 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=2.40 ms
^C
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2017ms
rtt min/avg/max/mdev = 2.397/3.272/4.745/1.047 ms

┌──(kali㉿kali2024)-[~]
└─$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=63 time=2.88 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=63 time=2.94 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=63 time=2.67 ms
64 bytes from 192.168.2.2: icmp_seq=4 ttl=63 time=3.00 ms
^C
--- 192.168.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3073ms
rtt min/avg/max/mdev = 2.666/2.872/3.003/0.126 ms

┌──(kali㉿kali2024)-[~]
└─$ 
```

WAN :



```
──(kali㉿kali2024blue)-[/etc/network]
─$ ping 192.168.3.2
ING 192.168.3.2 (192.168.3.2) 56(84) bytes of data.
4 bytes from 192.168.3.2: icmp_seq=1 ttl=63 time=3.83 ms
4 bytes from 192.168.3.2: icmp_seq=2 ttl=63 time=2.86 ms
4 bytes from 192.168.3.2: icmp_seq=3 ttl=63 time=2.84 ms
4 bytes from 192.168.3.2: icmp_seq=4 ttl=63 time=2.80 ms
4 bytes from 192.168.3.2: icmp_seq=5 ttl=63 time=3.16 ms
C
-- 192.168.3.2 ping statistics ---
 packets transmitted, 5 received, 0% packet loss, time 4014ms
tt min/avg/max/mdev = 2.800/3.097/3.828/0.387 ms

──(kali㉿kali2024blue)-[/etc/network]
─$ ping 192.168.2.2
ING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
4 bytes from 192.168.2.2: icmp_seq=1 ttl=63 time=2.62 ms
4 bytes from 192.168.2.2: icmp_seq=2 ttl=63 time=6.63 ms
4 bytes from 192.168.2.2: icmp_seq=3 ttl=63 time=2.87 ms
4 bytes from 192.168.2.2: icmp_seq=4 ttl=63 time=2.75 ms
C
-- 192.168.2.2 ping statistics ---
 packets transmitted, 4 received, 0% packet loss, time 3343ms
tt min/avg/max/mdev = 2.622/3.717/6.629/1.683 ms

──(kali㉿kali2024blue)-[/etc/network]
─$ 
```

OPT1 :

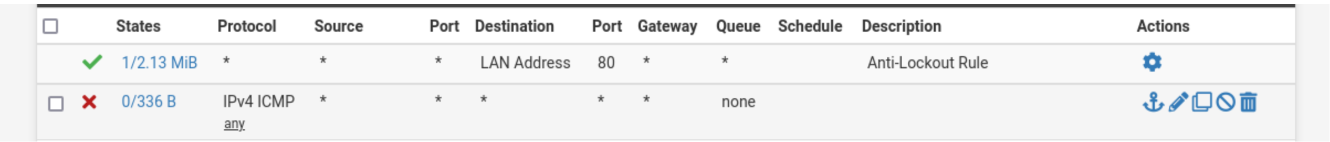


```
        valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$ ping 192.168.3.2
PING 192.168.3.2 (192.168.3.2) 56(84) bytes of data.
64 bytes from 192.168.3.2: icmp_seq=1 ttl=63 time=3.36 ms
64 bytes from 192.168.3.2: icmp_seq=2 ttl=63 time=3.02 ms
64 bytes from 192.168.3.2: icmp_seq=3 ttl=63 time=2.99 ms
64 bytes from 192.168.3.2: icmp_seq=4 ttl=63 time=3.26 ms
^C
--- 192.168.3.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.992/3.158/3.358/0.156 ms
ubuntu@ubuntu:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=10.9 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=2.69 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=2.90 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=63 time=3.07 ms

--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.689/4.902/10.945/3.491 ms
ubuntu@ubuntu:~$
```

2 Configuration du pare-feu/firewall pfsense (8 points)

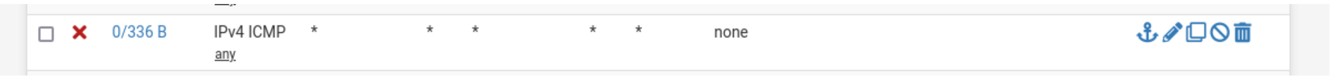
1) Ajoutez des r`egles au pare-feu pfsense pour bloquer toutes connexions entrantes et sortantes sur toutes les interfaces sauf pour l'IP de Kali purple qui doit garder l'acc`es a` pfsense. Quelles sont ces r`egles ? (captures ´ecran)

LAN :



□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1/2.13 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
□	✗	0/336 B	IPv4 ICMP any	*	*	*	*	*	none			⚓ ✎ ⧉ ⊘ 🗑

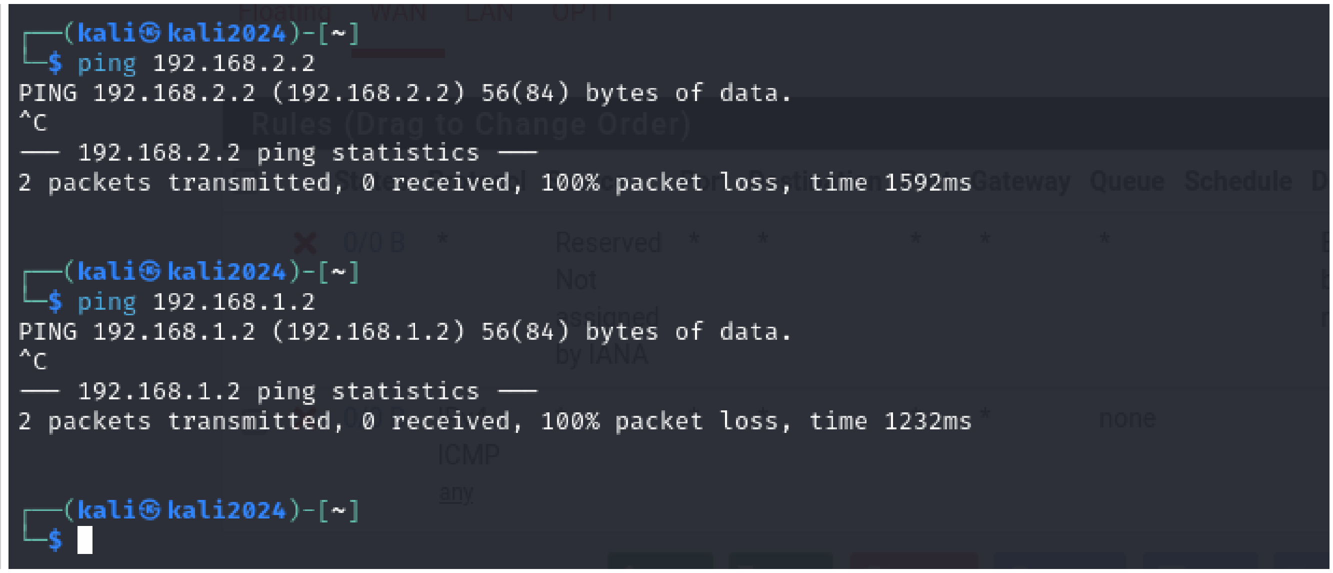
Others :



□	✗	0/336 B	IPv4 ICMP any	*	*	*	*	*	none			⚓ ✎ ⧉ ⊘ 🗑

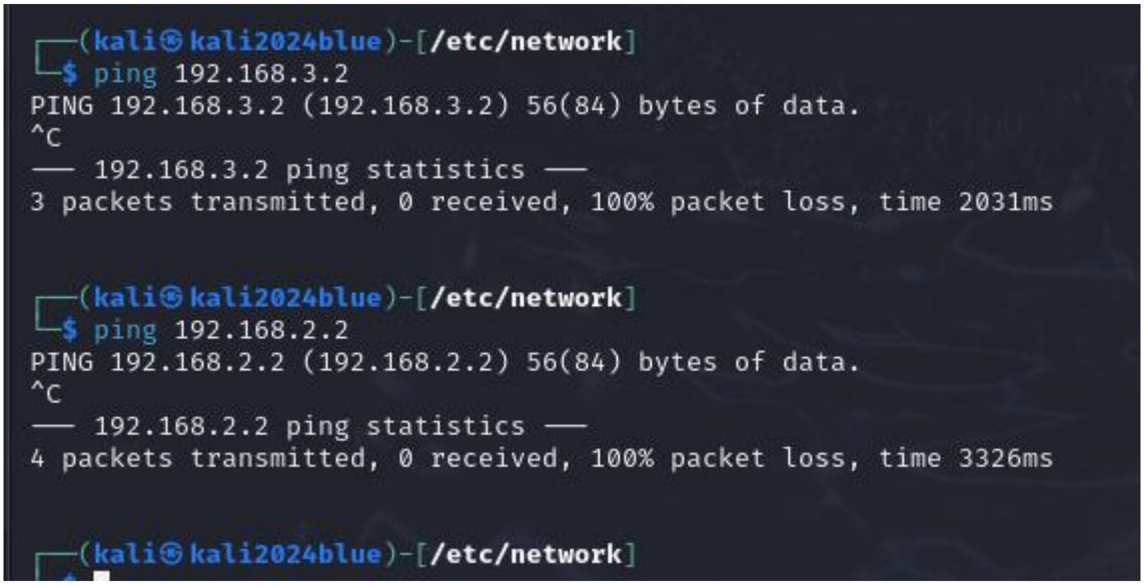
D´emontrez que cela fonctionne (capture ´ecran) :

LAN :



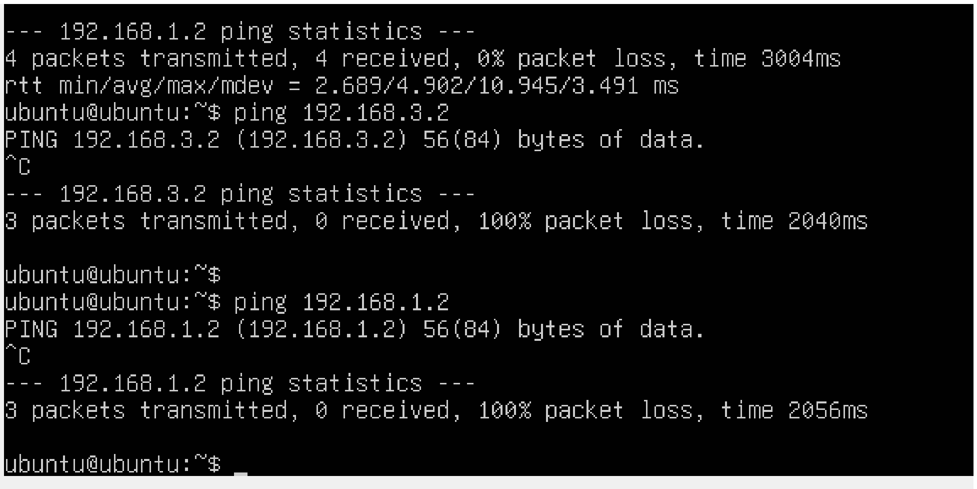
```
┌──(kali㉿kali2024)-[~]
└─$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
^C
── 192.168.2.2 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1592ms


┌──(kali㉿kali2024)-[~]
└─$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
── 192.168.1.2 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1232ms


┌──(kali㉿kali2024)-[~]
└─$ █
```

WAN :



```
┌──(kali㉿kali2024blue)-[/etc/network]
└─$ ping 192.168.3.2
PING 192.168.3.2 (192.168.3.2) 56(84) bytes of data.
^C
── 192.168.3.2 ping statistics ──
3 packets transmitted, 0 received, 100% packet loss, time 2031ms


┌──(kali㉿kali2024blue)-[/etc/network]
└─$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
^C
── 192.168.2.2 ping statistics ──
4 packets transmitted, 0 received, 100% packet loss, time 3326ms


┌──(kali㉿kali2024blue)-[/etc/network]
```

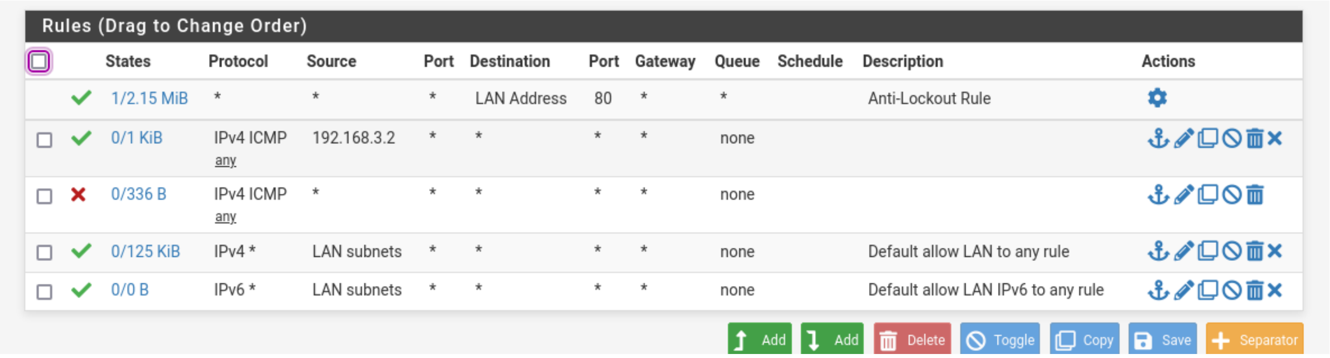
OPT1 :



```
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.689/4.902/10.945/3.491 ms
ubuntu@ubuntu:~$ ping 192.168.3.2
PING 192.168.3.2 (192.168.3.2) 56(84) bytes of data.
^C
--- 192.168.3.2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2040ms

ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2056ms

ubuntu@ubuntu:~$ _
```

2) Autorisez les requˆetes ICMP echo Ipv4 de LAN vers DMZ/WAN ainsi que de WAN vers DMZ. Quelles sont ces r`egles ?

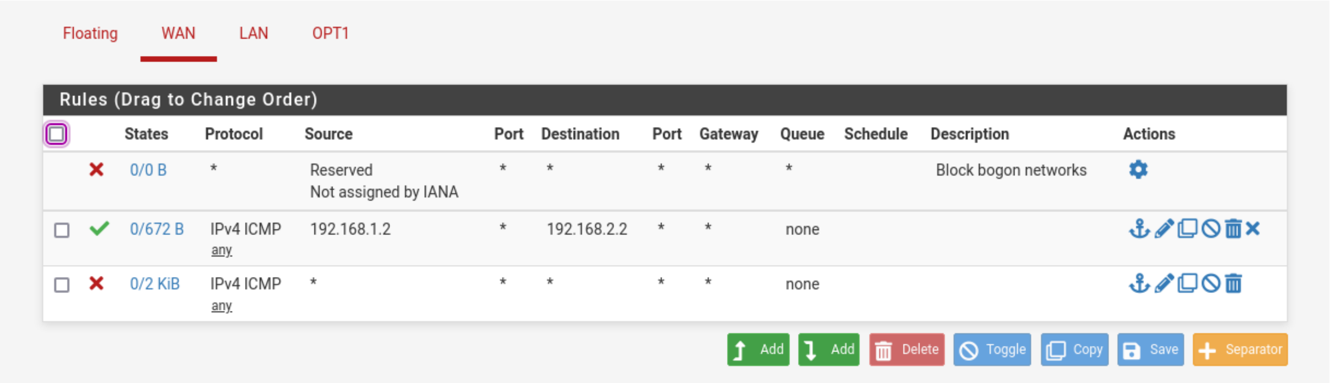
LAN :



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1/2.15 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
□	✓	0/1 KiB	IPv4 ICMP any	192.168.3.2	*	*	*	*	none			
□	✗	0/336 B	IPv4 ICMP any	*	*	*	*	*	none			
□	✓	0/125 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

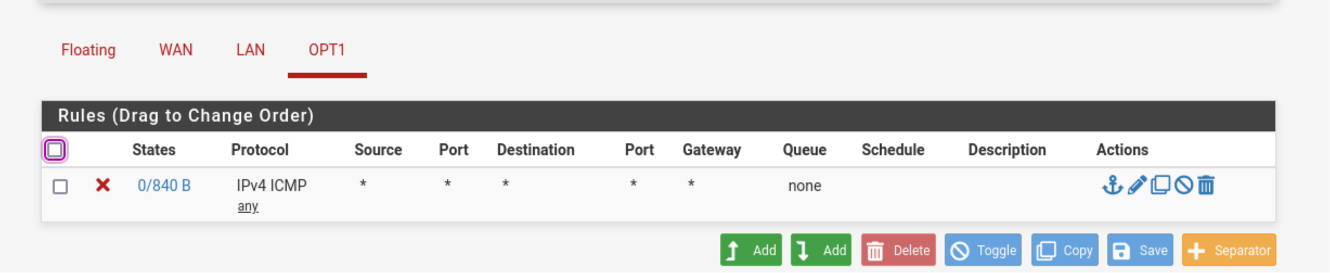
WAN :



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
□	✓	0/672 B	IPv4 ICMP any	192.168.1.2	*	192.168.2.2	*	*	none			
□	✗	0/2 KiB	IPv4 ICMP any	*	*	*	*	*	none			

OPT1 :

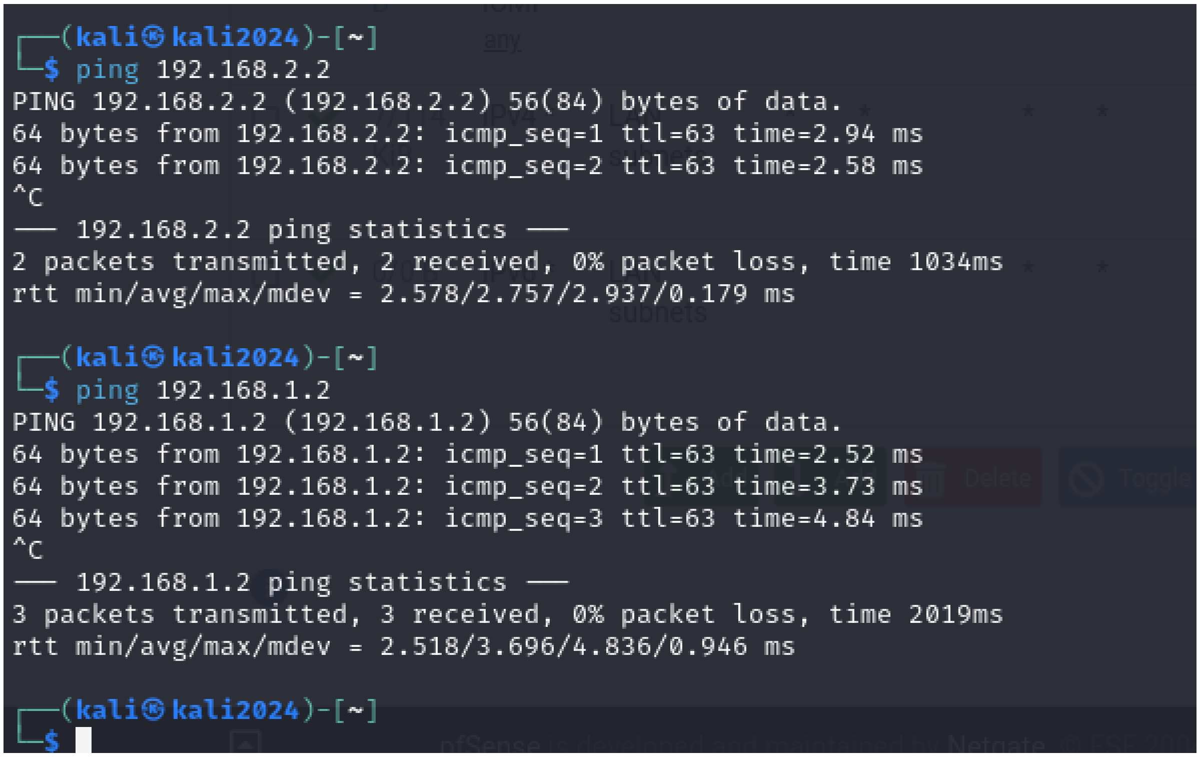


Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✗	0/840 B	IPv4 ICMP any	*	*	*	*	*	none			

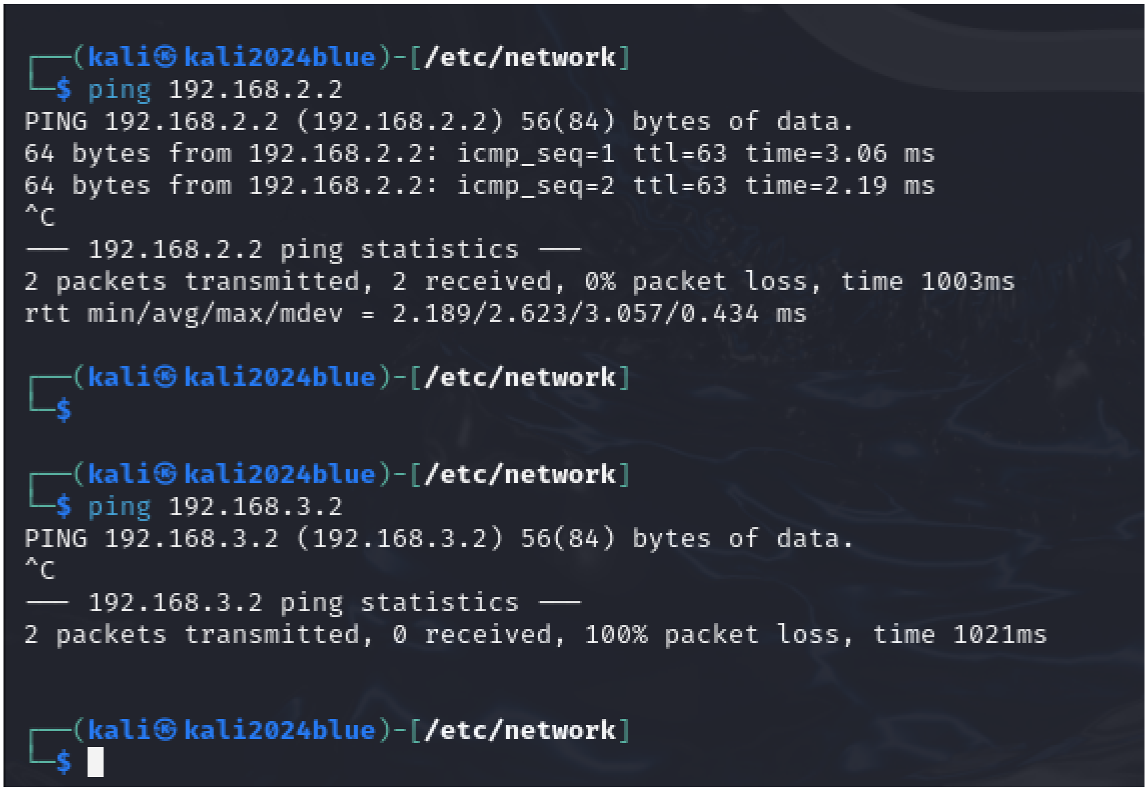
D´emontrez que cela fonctionne (capture ´ecran) :

LAN :



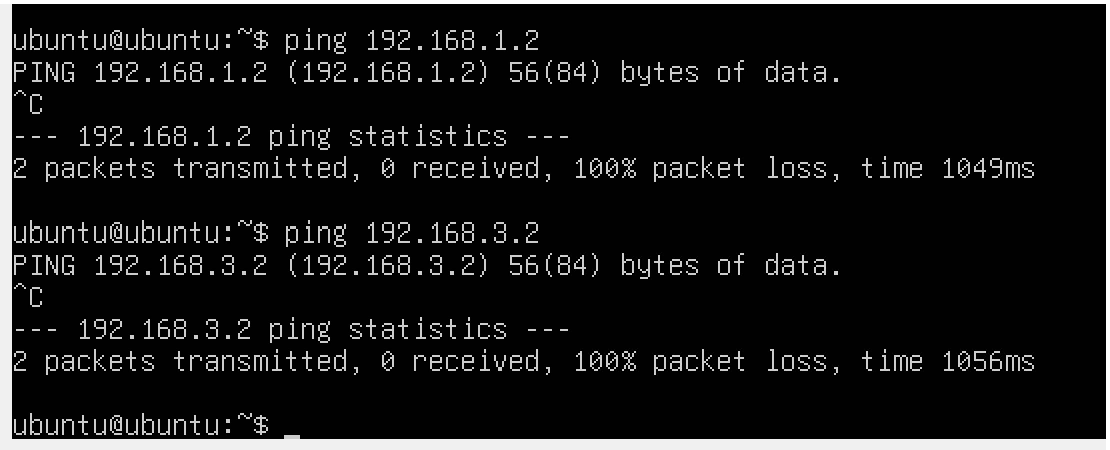
```
┌──(kali㉿kali2024)-[~]
└─$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=63 time=2.94 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=63 time=2.58 ms
^C
--- 192.168.2.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1034ms
rtt min/avg/max/mdev = 2.578/2.757/2.937/0.179 ms

┌──(kali㉿kali2024)-[~]
└─$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=2.52 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=3.73 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=4.84 ms
^C
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2019ms
rtt min/avg/max/mdev = 2.518/3.696/4.836/0.946 ms

┌──(kali㉿kali2024)-[~]
└─$ 
```

WAN :



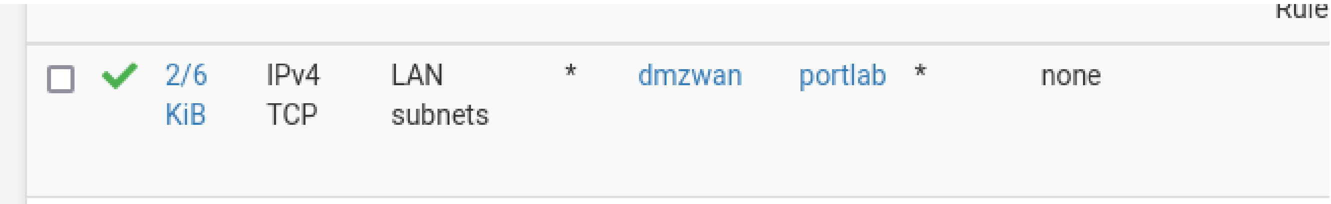
```
┌──(kali㉿kali2024blue)-[/etc/network]
└─$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=63 time=3.06 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=63 time=2.19 ms
^C
--- 192.168.2.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 2.189/2.623/3.057/0.434 ms

┌──(kali㉿kali2024blue)-[/etc/network]
└─$ 

┌──(kali㉿kali2024blue)-[/etc/network]
└─$ ping 192.168.3.2
PING 192.168.3.2 (192.168.3.2) 56(84) bytes of data.
^C
--- 192.168.3.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1021ms


┌──(kali㉿kali2024blue)-[/etc/network]
└─$ 
```

OPT1 :



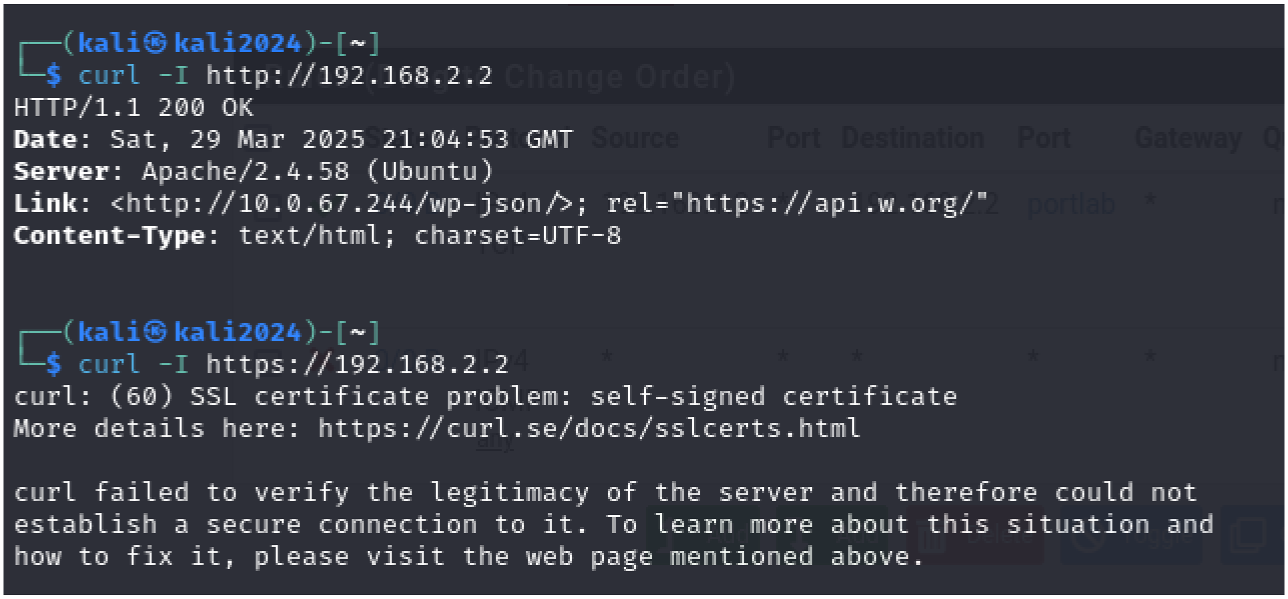
```
ubuntu@ubuntu:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1049ms

ubuntu@ubuntu:~$ ping 192.168.3.2
PING 192.168.3.2 (192.168.3.2) 56(84) bytes of data.
^C
--- 192.168.3.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1056ms

ubuntu@ubuntu:~$ _
```

3) Autorisez les acc`es TCP IPv4 de LAN vers WAN et DMZ sur les ports 80 et 443 uniquement. Quelle est cette r`egle ?

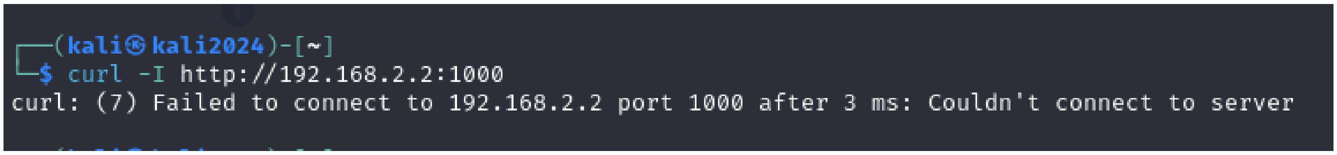


										Rule
□	✓	2/6 KiB	IPv4 TCP	LAN subnets	*	dmzwan	portlab	*	none	

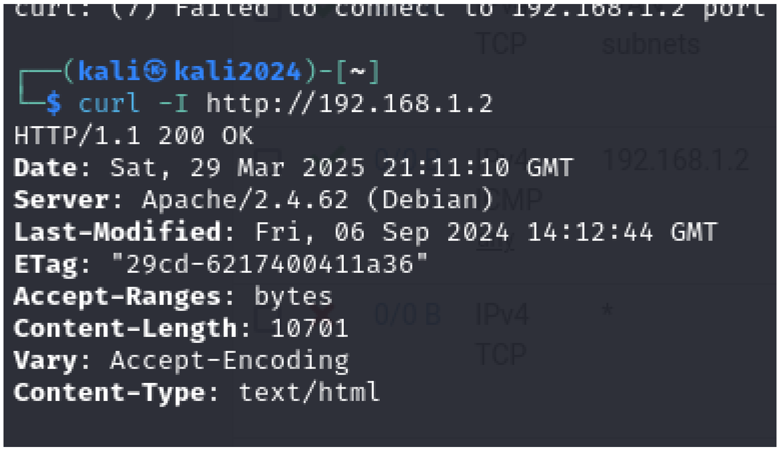
D´emontrez que cela fonctionne (capture ´ecran) :



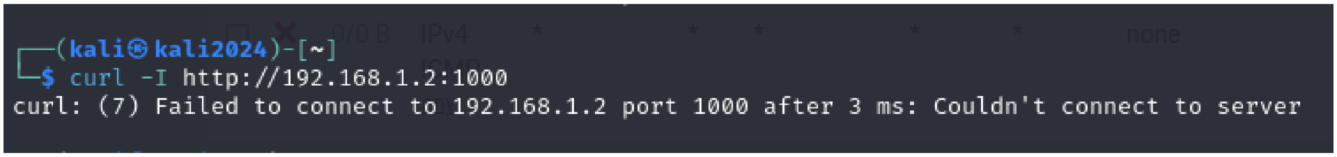
```
┌──(kali㉿kali2024)-[~]
└─$ curl -I http://192.168.2.2
HTTP/1.1 200 OK
Date: Sat, 29 Mar 2025 21:04:53 GMT
Server: Apache/2.4.58 (Ubuntu)
Link: <http://10.0.67.244/wp-json/>; rel="https://api.w.org/"
Content-Type: text/html; charset=UTF-8


┌──(kali㉿kali2024)-[~]
└─$ curl -I https://192.168.2.2
curl: (60) SSL certificate problem: self-signed certificate
More details here: https://curl.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.
```



```
┌──(kali㉿kali2024)-[~]
└─$ curl -I http://192.168.2.2:1000
curl: (7) Failed to connect to 192.168.2.2 port 1000 after 3 ms: Couldn't connect to server
```

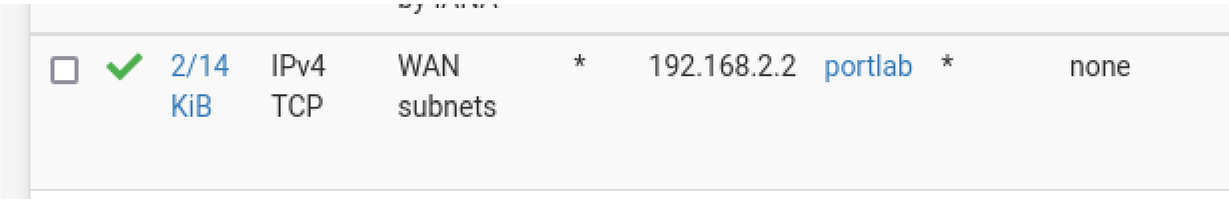


```
curl: (7) Failed to connect to 192.168.1.2 port

┌──(kali㉿kali2024)-[~]
└─$ curl -I http://192.168.1.2
HTTP/1.1 200 OK
Date: Sat, 29 Mar 2025 21:11:10 GMT
Server: Apache/2.4.62 (Debian)
Last-Modified: Fri, 06 Sep 2024 14:12:44 GMT
ETag: "29cd-6217400411a36"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Content-Type: text/html
```



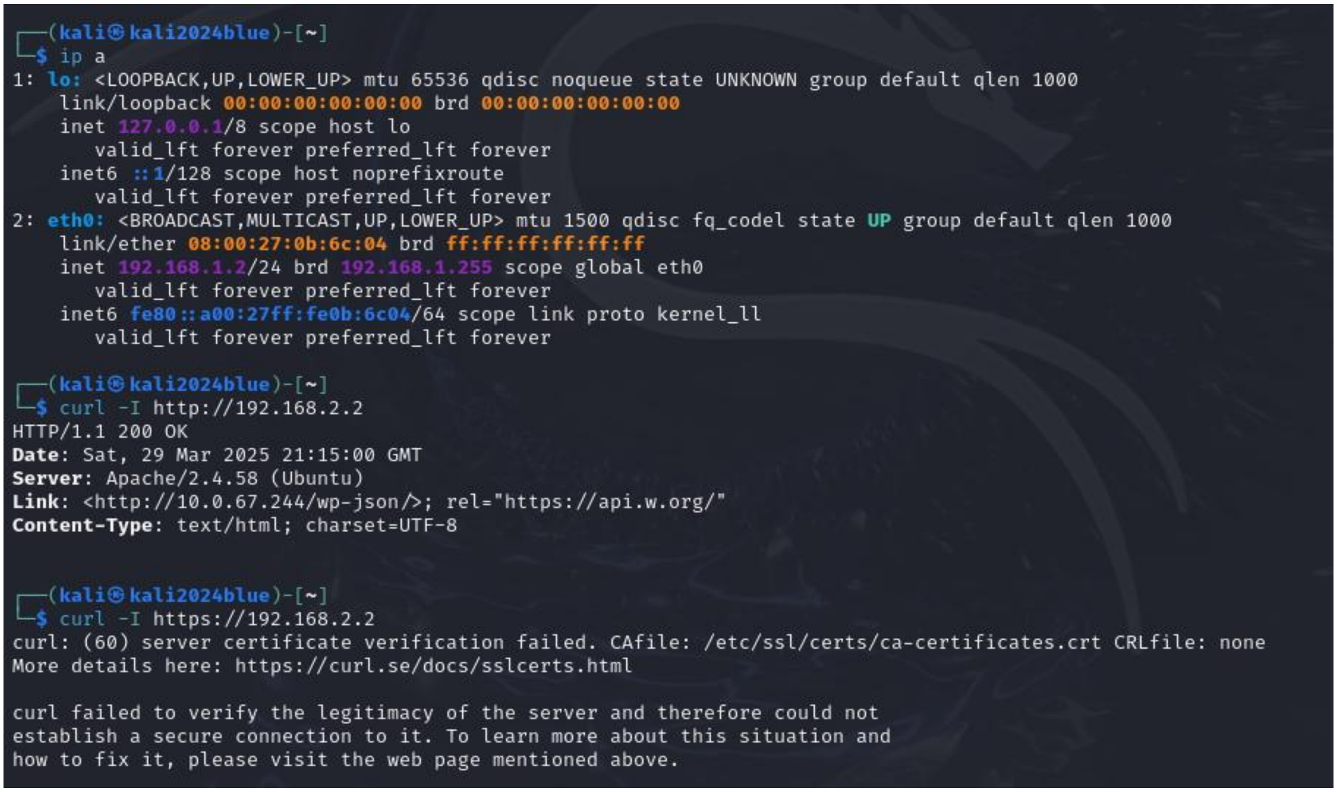
```
┌──(kali㉿kali2024)-[~]
└─$ curl -I http://192.168.1.2:1000
curl: (7) Failed to connect to 192.168.1.2 port 1000 after 3 ms: Couldn't connect to server
```

4) Autorisez les acc`es TCP Ipv4 de WAN vers DMZ sur les ports 80, 443. Quelle est cette r`egle ? D´emontrez que cela fonctionne (capture ´ecran) :



☐	✓	2/14 KiB	IPv4 TCP	WAN subnets	*	192.168.2.2	portlab	*	none

5)



```
┌──(kali㉿kali2024blue)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:0b:6c:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.2/24 brd 192.168.1.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe0b:6c04/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(kali㉿kali2024blue)-[~]
└─$ curl -I http://192.168.2.2
HTTP/1.1 200 OK
Date: Sat, 29 Mar 2025 21:15:00 GMT
Server: Apache/2.4.58 (Ubuntu)
Link: <http://10.0.67.244/wp-json/>; rel="https://api.w.org/"
Content-Type: text/html; charset=UTF-8


┌──(kali㉿kali2024blue)-[~]
└─$ curl -I https://192.168.2.2
curl: (60) server certificate verification failed. CAfile: /etc/ssl/certs/ca-certificates.crt CRLfile: none
More details here: https://curl.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.
```

Ce laboratoire est termin´e